press the flash hook to move back and forth between two legs of a call repeatedly without ever generating a Change message. The interim standard does not ensure that the government receives this critical information about the direction and destination of each communication within the call. As a result, TIA is fundamentally mistaken when it asserts (TIA Comments at 49) that the only additional information provided under the government's proposed rule is "the identity of the actual keys pressed" by the subject.

TIA also argues that Section 103 does not obligate a carrier to provide law enforcement with access to "local" subject-initiated signaling activity, such as signaling activity internal to a PBX, that is not detected by the carrier's network. TIA Comments at 50. This argument is based on a misunderstanding of the government's petition and proposed rule. The government is not asking for carriers to provide access to local subject-initiated signaling activity that is not detected by their networks. See DOJ/FBI Petition, Appendix 1, § 64.1708(c)(1). TIA's objections are therefore immaterial.

Finally, BellSouth states that in "some" switch implementations, the detection and collection of off-hook signals and digit dialing occurs in a line module that is separate and distinct from the main processor of the switch. BellSouth Comments at 11. BellSouth asserts that making this information available to the main processor so that it can be sent to law enforcement "may" require fundamental modifications to the architecture of such switches. Ibid. But the information must be delivered to the main processor at some point if the switch is to carry out the necessary call processing successfully. Moreover, even if BellSouth's claim were true for particular switching platforms, and even if the nature of the needed modifications meant that the information was not "reasonably available" to carriers using those platforms, BellSouth itself does not suggest that all (or

even most) platforms would require this kind of redesign. Yet the interim standard excuses all carriers from providing information about subject-initiated dialing and signaling activity, regardless of the particular platform they are using. As explained above, the interim standard is deficient unless it ensures that all carriers who comply with it are delivering the call content and call-identifying information that they are required to provide under Section 103 of CALEA. See pp. 12-13 supra. The fact (if it is a fact) that call-identifying information may not be "reasonably available" to certain carriers does not justify an industry standard that relieves all carriers from the obligation to provide such information.

E. Information on Participants in Multi-Party Calls

The interim standard does not require carriers to provide any message or signaling information indicating that a party has joined a multi-party call, been placed on hold, or dropped from the call. See DOJ/FBI Petition ¶ 73. Without such information, law enforcement would not know who joins or leaves a conference call, whether the subject alternated between legs of the call, or which parties may have heard or said particular communications during the course of the call. Id. ¶ 75. For reasons given in the government's petition, information that identifies party "joins," "drops," and "holds" in multi-party calls constitutes "call-identifying information" under CALEA, and access to such information has potentially great investigatory and evidentiary value to law

enforcement. Id. ¶¶ 75-78.[29] The government's proposed rule therefore provides for the delivery of "party join," "party drop," and "party hold" messages.

TIA argues that the interim standard already provides law enforcement with the information that would be provided by the proposed Party Join and Party Drop messages. TIA Comments at 52-53. TIA asserts that the information covered by the Party Join message is already provided by the interim standard's Origination, TerminationAttempt, and Change messages. Ibid. TIA further asserts that the information sought by the Party Drop message is already provided by the Release message. Id. At 52-53. These assertions are incorrect.

The combination of the Origination and Change messages does not serve as an effective proxy for the Party Join message. As already explained in connection with the issue of subject-initiated dialing and signaling activity, the Change message is tied to changes in call identities rather than changes in party identities. See pp. 48-49 supra. As a result, a Change message will not necessarily be generated when a subject joins two parties into a conference call. Indeed, the interim standard itself expressly demonstrates this result. See J-STD-025, Annex D.10.1, Table 28, Step 8

---

[29] Several commenters note that, even if a law enforcement agency receives party join and party hold information, it will not necessarily be able to determine or prove that a joined party was actually listening to the conversation. See TIA Comments at 54; AT&T Comments at 10. That is true, but it hardly shows that party join and party drop messages lack evidentiary and investigatory value. In some instances, it may be just as important to law enforcement to know who was not "on the line" at the time of a particular communication as to know who was. Moreover, simply knowing that a particular statement by a subject was directed to one party, rather than to another party, may be significant for the course of an investigation even if law enforcement cannot be completely certain that the party heard the statement. In any event, CALEA does not condition the assistance capability requirements of Section 103 on the telecommunications industry's appraisal of the law enforcement value of particular information; as long information comes within the scope of Section 103, carriers are obligated to provide it to law enforcement.

(no Change message generated when subject joins party A and party B). The combination of the TerminationAttempt message and Change message suffers from the same defect.

Turning from party joins to party drops, the Release message is not a substitute for the Party Drop message because the interim standard does not require a carrier to send the Release message when a single call leg or call appearance is released. Instead, it makes the delivery of the Release message for such events discretionary. See J-STD-025 § 5.4.8 ("The Release message may be triggered when a call leg or call appearance is released") (emphasis added). The Release message is mandatory, rather than discretionary, only when an entire call ends. See id. ("The Release message shall be triggered when * * * a completed circuit-mode call is released") (emphasis added). If a particular manufacturer uses a single call identity for all legs of a conference call, the Release message therefore will not be sent until the conference call is completed; the dropping of a single party from the conference call will not generate the message.

With respect to party holds, TIA concedes that the interim standard does not provide any message that corresponds to the proposed Party Hold message. However, TIA argues that information about party holds does not constitute "call-identifying information." TIA Comments at 53-54.[30] Other commenters go well beyond TIA's position by arguing that "call-identifying information" does not include any of the information sought by law enforcement regarding party joins, drops, and holds. See, e.g. CDT Comments at 45; USTA Comments at 4; BellSouth Comments at 9.

---

[30] TIA also states that, to the extent that a hold key is not detected by a carrier's network, the hold information is not "reasonably available" to the carrier. TIA Comments at 54. TIA is evidently discussing "local" signaling activity (such as signaling internal to a PBX). As explained above, the government is not asking carriers to provide information about such local signaling activity. See p. 49 supra.

The legal analysis underlying these comments suffers from two closely related shortcomings. First, the statutory definition of "call-identifying information" covers all dialing or signaling information that identifies "the origin, direction, destination, or termination of each communication generated or received by a subscriber * * * ." 47 U.S.C. § 1001(2) (emphasis added). When a subscriber's facilities are supporting a multi-party call, a single call may (and often will) involve more than one "communication." For example, if the subject holds a conversation with one party, then joins another party for a conference call, then drops the first party and continues speaking with the second party, each discussion constitutes a separate "communication." The definition of "call-identifying information" means that the carrier must provide information that identifies the origin, direction, destination, and termination of each of these communications, not simply the call as a whole. (Tellingly, when TIA discusses the Party Hold message (TIA Comments at 53-54), TIA finds it necessary to replace "each communication" with "[a] communication.")

Second, the commenters once again rely on an unduly restrictive reading of "origin, direction, destination, or termination." As explained in the government's petition, each time a subject adds a party to a conference call or a party is dropped or placed on hold, notification of the event identifies the subject's direction of each communication making up the conference call and the destination of each communication. See DOJ/FBI Petition ¶ 78. As a result, party join, party drop, and party holding information constitutes "information that identifies the * * * direction [and] destination * * * of each communication" involved in the call.

In the government's rulemaking petition, we noted that law enforcement has not historically had the technical capability to obtain information showing that joined parties have been placed on hold or dropped from multi-party calls, because such information resides in the switch and cannot

be accessed from the local loop. See DOJ/FBI Petition ¶ 77. Several commenters suggest that the lack of traditional access to this information places it outside the bounds of Section 103(a)(2). See, e.g., USTA Comments at 4; PrimeCo Comments at 14. As already discussed, however, traditional capabilities are not dispositive regarding the scope of CALEA. See pp. 10-11 supra. Here, the statutory language is sufficiently clear, and the investigatory and evidentiary weight of the information sufficiently integral to the law enforcement goals underlying CALEA, to support the conclusion that carriers are obligated to provide access to the information.

BellSouth and USTA assert that delivery of party join, party drop, and party hold messages to law enforcement at the subscriber's switch may be technically difficult when a conference call is handled by a conferencing bridge element that is remote from the switch. BellSouth Comments at 9-10; USTA Comments at 5.[31] However, in the case of conventional three-way or six-way conference call services, the conference call feature is supported in the switch. And for some platforms, even the kind of conferencing bridge service described by BellSouth is available within the switch. At the very most, therefore, the comments indicate that party join, party drop, and party hold messages may not be "reasonably available" in all circumstances. The interim standard, however, does not require carriers to provide these messages in any circumstances. For that reason, the interim standard is plainly deficient.

---

[31] These comments assume that the intercept access point (IAP) is necessarily at the switch. There is no basis in CALEA for that restrictive assumption, and the interim standard itself does not make such an assumption. For example, the interim standard requires Home Location Registers (HLRs), which are not necessarily part of the switch, to report serving system messages and feature information. See J-STD-025 § 3, p. 8 (definition of IAP); id. Annex A, Figure 12.

F. Notification of Network-Generated In-Band and Out-of-Band Signaling

When a call attempt is made to or from a subscriber's equipment, facilities, or services, the carrier's network generates in-band or out-of-band signaling that identifies call progress. These signals may be presented to the subject as audible tones, visual indicators, or alphanumeric display information. For outgoing call attempts, these signals indicate (for example) whether the call attempt ended with a busy signal, ringing, or before the network could complete the call. For incoming call attempts, these signals indicate (for example) whether the subject's telephone received a call waiting tone or was alerted to the redirection of a call to voice mail by a "stutter" tone or a message-waiting light. Collectively, these signals show how the network treated a call attempt: whether or not it was completed, how the call may have been redirected or modified, and how the call ended.

The interim standard does not require carriers to provide law enforcement with notification of network-generated call progress signals. For reasons set forth in the government's petition, carriers are obligated to provide access to this information under Section 103(a)(2) of CALEA, and the omission of the information renders the interim standard deficient. See DOJ/FBI Petition ¶¶ 80-81.

1. A number of commenters assert that network-generated call progress signals are not call-identifying information or, more narrowly, that particular signals (such as busy tones and call waiting indicators) are not. See, e.g., TIA Comments at 56-57, CDT Comments at 45-46; BellSouth Comments at 11; Nextel Comments at 11; SBC Comments at 12; AT&T Comments at 11-12. As explained in our petition, however, all of the signals at issue here identify the "direction," "destination," and/or "termination" of a communication. DOJ/FBI Petition ¶ 81. A call attempt may

"terminate" with ringing (without an answer), with a busy tone, or with a trunk busy signal; signaling such as this conveys information on call termination and therefore constitutes call-identifying information. Similarly, a network-generated call-waiting tone or a "stutter" tone identifies the "direction" or "destination" of the call and is therefore likewise call-identifying information.

Several commenters assert that the definition of "call-identifying information" excludes information identifying how a call attempt terminates. See, e.g., AT&T Comments at 12. But nothing in the language of the statutory definition suggests such a limitation. A call attempt that ends with a busy signal and one that ends with ringing have different "terminations"; only by learning the network-generated signal can law enforcement identify the specific termination of the call attempt. Here, as elsewhere, the commenters are relying on an unduly restrictive reading of "call-identifying information," one that would exclude significant information to which law enforcement traditionally has had access over the local loop.[32]

TIA and several other commenters state that when signaling information is generated by a remote network switch, such as a busy signal generated in an outgoing long-distance call, the signaling information is not "reasonably available" to the subscriber's local carrier, and therefore is not within the local carrier's assistance capability obligations under Section 103(a)(2), because the local carrier's switch is not equipped to detect busy signals and other tones generated by remote switches. See TIA Comments at 58-59; USTA Comments at 5; BellSouth Comments at 12; SBC

---

[32] The government does not contend, as TIA suggests (TIA Comments at 59-60), that network-generated signals like ringing constitute call-identifying information because they can be used by criminals to convey pre-arranged messages. Ringing and other tones can indeed be used for such purposes, and that is one reason why it is important for law enforcement to have access to them, but they are call-identifying information for a different reason -- because they identify the termination of the call.

Comments at 12. These comments reflect a misunderstanding of the scope of the government's petition. The government is not asking a carrier to provide notification of in-band and out-of-band signaling generated outside the carrier's own network. The government's proposed rule is limited to in-band and out-of-band signaling "from the subscriber's service" -- that is, signaling generated by the carrier providing the subscriber's service, not signaling generated by another carrier. See DOJ/FBI Petition, Appendix 1 (§ 64.1708(d)); see also id. § 64.1708(d)(1) ("accessing system"). As a result, when (for example) a subscriber places a long-distance call and receives a busy signal generated by the called party's carrier, the subscriber's carrier would not be required to deliver a notification message of the busy signal to law enforcement.

2. In addition to arguing that network-generated call progress signals are not "call-identifying information," TIA argues that the interim standard already provides much of the information sought by the government. See TIA Comments at 56-61. However, TIA considerably overstates the comprehensiveness and effectiveness of the interim standard.

TIA suggests that "most" audible signaling tones (such as busy signals) are available to law enforcement over call content channels, thereby eliminating the need for delivery of a notification message regarding audible tones. TIA Comments at 57-58; see also USTA Comments at 5-6; PrimeCo Comments at 16-17. However, the interim standard requires delivery of call content to law enforcement only between call completion (answer) and call release. See J-STD-025 § 4.5.1 There is no requirement that the carrier deliver call content on incoming calls before they are answered. Instead, the interim standard provides only that "[c]all content may be delivered before answer and may include call progress tones or announcements." Ibid. (emphasis added).

In addition, even when call content is being delivered to law enforcement, the call content channel running from the switch to law enforcement may not reflect the call progress tones being delivered from the switch to the subscriber's terminal. For example, wireless and ISDN networks send out-of-band "alert" messages that tell a subscriber's terminal to ring or generate some other signal. Law enforcement cannot detect the resulting tones by monitoring the call content channel, because the tones are not being generated at the switch.[33]

TIA also suggests that the interim standard's existing data messages convey all of the call-identifying information that is conveyed by audible tones such as busy signals and stutter dial tones. See TIA Comments at 56-57. However, the data messages cited by TIA provide no information about how the call terminated. Nor do they disclose what signals, if any, were presented to the subject -- for example, whether the subject received notification of an incoming call through a call waiting tone. TIA's argument in this regard depends entirely on its restrictive reading of the meaning of "call-identifying information."

With respect to alphanumeric display information, TIA states that the TerminationAttempt message provides the telephone number of the calling party. TIA Comments at 60. But just as the TerminationAttempt message is an inadequate substitute for audible tones, so too is it an inadequate substitute for alphanumeric display information. For example, an alphanumeric display may notify the subject that a call has been redirected to the subscriber's voice mail box. Neither the TerminationAttempt message nor the Redirection message would disclose that a message had been

---

[33] When audible call progress tones are available over a call content channel, the government does not contend that a carrier must provide notification of the tones over a call data channel in order to comply with Section 103. Nevertheless, for reasons set forth above (see pp. 44-45 supra) and in the government's petition (DOJ/FBI Petition ¶¶ 83-85), the Commission properly may include delivery over a CDC in standards adopted by the Commission.

left for the subject. And if a calling party can access the subject's voice mail box directly, rather than by being redirected from the subject's phone number, law enforcement will have no idea that the call has even been made unless it receives notification of the alphanumeric information alerting the subject to the call.

G. Timely Delivery of Call-Identifying Information

1. Section 103(a)(2) of CALEA obligates carriers to make call-identifying information available to law enforcement "before, during, or immediately after the transmission of a wire or electronic communication" and "in a manner that allows it to be associated with the communication to which it pertains." 47 U.S.C. § 1002(a)(2). Law enforcement's ability promptly to obtain call-identifying information and correlate it with the communication to which it pertains can be crucial, directly affecting law enforcement's ability to respond in emergency and life-threatening cases, as well as enabling law enforcement to "minimize" the interception of non-criminal communications to protect privacy. Yet, as explained in the government's petition, the interim standard imposes no requirement with regard to when call-identifying information must be delivered to law enforcement. This omission renders the interim standard deficient.

TIA asserts that law enforcement's claimed need for timely delivery of call-identifying information rests solely on "colorful" but "imaginary" examples that the government has "conjure[d] up." TIA Comments at 63-64. This assertion betrays a striking insensitivity to, and ignorance of, the actual state of affairs in the realm of electronic surveillance. Although the Commission undoubtedly can appreciate the real-world consequences of law enforcement's lack of timely access to call-identifying information without being presented with a litany of examples, TIA's comments make an illustrative response necessary.

At approximately 11:30 p.m. on January 25, 1996, a 35 year-old woman was abducted near her home in Queens, New York. Her kidnapers took her to a basement and telephoned her husband in China and her relatives in New York City, demanding $38,880 in ransom. Her husband heard her screaming in the background as the kidnapers made their demand. After being alerted to the situation, the New York City Police Department (NYPD) obtained court authorization and installed a wiretap and a trap and trace device on the victim's New York relatives' telephone -- a standard strategy in kidnaping cases. However, the carrier was unable to trace the kidnapers' calls quickly enough through its switches and trunk lines to identify the number from which the calls were being made. For days, the NYPD was able to listen to the kidnapers' threatening calls to the victim's relatives but could not determine where the woman was being held. As the kidnapers' deadline for payment neared, their calls became progressively more menacing. When the NYPD finally was able to determine the kidnapers' number, go to the location where the woman was being held, and rescue her, she had been held for thirteen days. Her kidnapers had raped and beaten her daily during this period. See Declaration of Detective John Ross (attached); Dan Morrison, 13 Days in Hell: City, China cops rescue kidnaping, rape victim, NEWSDAY, Feb. 9, 1996, at A3.

In a related vein, AT&T states that it is "patently absurd" to suggest that carriers would delay the delivery of call-identifying information to law enforcement for hours or days. AT&T Comments at 14 n.48. We wish this were so. Turning again to the experience of the NYPD, one New York City carrier's standard time frame for delivering call-identifying information to law enforcement is two days after the call has occurred. The NYPD has heard subjects advise each other to switch to digital technology in order to foil interceptions, and has repeatedly been frustrated in its efforts to collect the pertinent information in time to make effective use of it. See Declaration of Detective

John Ross (attached). These real-life examples should make it abundantly clear that law enforcement's need for timely delivery of call-identifying information is anything but "imaginary."

2. Many of the comments are directed not at the underlying need for timely delivery of call-identifying information, but rather at the details of the specific timing requirements in the government's proposed rule. These comments fail to come to terms with the basic point of the government's petition -- namely, that the interim standard is deficient because it lacks any requirements for timely delivery. The Commission's first order of business should be to ask whether an industry standard that places no requirements at all on carriers regarding how quickly call-identifying information must be delivered to law enforcement is adequate to ensure that carriers meet their statutory obligations under Section 103(a)(2). In our view, that question admits of only one answer.

To the extent that the commenters do address the underlying deficiency issue, their arguments are misconceived. The commenters argue that the interim standard is not deficient because Section 103 does not itself impose any "explicit maximum delivery time." TIA Comments at 66; see also CTIA Comments at 17; AirTouch Comments at 20; AT&T Comments at 14. But all of the assistance capability requirements of Section 103 are framed in general, rather than specific, terms; the whole point of the standard-setting process is to give specific content to the general provisions of Section 103 by identifying more precisely what steps are required for a carrier to meet its underlying assistance capability obligations. Omissions from the interim standard therefore can hardly be defended on the theory that there are no correspondingly precise terms in Section 103 itself. A fortiori, the lack of a specific timing requirement in Section 103 cannot excuse the absence of any timing requirement in the interim standard.

Equally misguided is the argument that any specification of a time frame for delivery of call-identifying information would be "arbitrary." USTA Comments at 6; BellSouth Comments at 13; SBC Comments at 12. A specified maximum time for the delivery of call-identifying information would be no more "arbitrary" than any other specific item already included in the interim standard.

The assertion that the government's proposal represents an attempt at "dictating" a specific system design, in violation of Section 103(b)(1) of CALEA, is mistaken. See SBC Comments at 12. Simply requiring that call-identifying information be delivered within a particular time frame hardly constitutes "requir[ing] any specific design" of a carrier's equipment or system configuration (47 U.S.C. § 1002(b)(1)), any more than requiring the delivery of a specified data message does so. Carriers choosing to satisfy their obligations by means of the Commission's standards will remain free to provide this capability using any equipment or design they prefer. Moreover, as noted above, no carrier is mandated to comply with the specific provisions of the Commission's standards if it can meet its assistance capability obligations by other means.

The assertion that any maximum time frame for the delivery of call-identifying information would ignore the diversity of carriers and compliance solutions in the industry, or the possibility of congestion on the network (see, e.g., AirTouch Comments at 21; PrimeCo Comments at 18), must be rejected. The specific time frame recommended in the government's proposed rule -- three seconds after the associated call event -- was deliberately selected with a view towards making compliance feasible for diverse carriers utilizing various solutions, operating in an environment which may at times face network congestion. In fact, the vast majority of carriers routinely and normally deliver call-identifying information as necessary to perform call setup and takedown in well under three seconds, commonly in a matter of microseconds. The fact that the suggested

standard only requires 99% reliability with regard to timely delivery represents a further attempt to take these factors into account.[34]

Finally, TIA argues that requiring delivery of call-identifying information within three seconds of the associated event conflicts with the language in Section 103(a)(2) allowing delivery of call-identifying information "immediately after" the transmission of a wire or electronic communication. TIA Comments at 65. In TIA's view, this language shows that a carrier need not provide call-identifying information until immediately after the completion of "the call," and thus if a call lasts for several hours (as many types of calls involving criminal activity -- especially illegal gambling -- typically do), call-identifying information pertaining to events that took place at the beginning of the call or during the course of the call may be delivered en masse hours later, when the call is completed. See ibid. ("Congress certainly envisioned telephone calls lasting longer than three seconds").

This argument cannot be squared with the actual terms of Section 103(a)(2). First, Section 103(a)(2) does not tie a carrier's timing obligations to "the call," as TIA's argument suggests. Instead, the carrier must deliver call-identifying information "before, during, or immediately after the transmission" of the "wire or electronic communication" to which the call-identifying information "pertains." 47 U.S.C. § 1002(a)(2)(A) (emphasis added). A single call may encompass any number of "communications." See 18 U.S.C. § 2510(1) (defining "wire communication"); id.

---

[34] As Ameritech notes, an industry standards committee is currently considering a proposal for delivering call-identifying information within "a maximum of three (3) seconds at least 98% of the time." Ameritech Comments at 8. This casts considerable doubt on other commenters' objections to the feasibility of delivering call-identifying information within a maximum of three seconds at least 99% of the time.

§ 2510(12) (defining "electronic communication"); 47 U.S.C. § 1001(1) (incorporating definitions in 18 U.S.C. § 2510).

Second, Section 103(a)(2) requires delivery of call-identifying information before, during, or immediately after "the transmission of" each communication. 47 U.S.C. § 1002(a)(2) (emphasis added). TIA's argument effectively replaces "transmission" with "completion," so that the delivery obligation does not arise until the call is over. The transmission of a communication is a continuous, ongoing process, not something that occurs only when the communication ends, and the timely delivery obligations of Section 103(a)(2) are correspondingly ongoing.

Finally, TIA's argument ignores Section 103(a)(2)(B), which requires call-identifying information to be delivered "in a manner that allows it to be associated with the communication to which it pertains." 47 U.S.C. § 1002(a)(2)(B). When a call continues for lengthy period, law enforcement cannot associate the call-identifying information with particular communications in a meaningful way if delivery of the call-identifying information is postponed -- as the interim standard permits it to be -- until hours later. As explained in the government's petition, for example, a communication that occurs at the beginning of an hour-long call might involve a direction to carry out a killing immediately -- if law enforcement cannot obtain the call-identifying information pertaining to this utterance until an hour or more later, it may well be unable to prevent the murder. Requiring the prompt delivery of the pertinent call-identifying information will ensure that law enforcement can "associate" the information with the communication in a meaningful and effective way.

3. In order to ensure that law enforcement can correlate individual "wire or electronic communications" with their respective call-identifying information, the government's proposed rule

also provides for an accuracy rate of 100 milliseconds for the time stamps that show when particular triggering events occurred. The few objections raised against this proposal cast no doubt on our observation that the interim standard suffers from a deficiency in this respect, nor do they identify any valid reason for the Commission to reject our proposed solution.

TIA asserts that the accuracy rate of 100 milliseconds is not "reasonably available" because an event can occur in a part of the network far distant from the place at which the time-stamp is affixed. See TIA Comments at 67. This comment appears to misunderstand our recommendation. We seek to be assured of the accuracy of the recording only of events that occur when a network element acts upon a subscriber's input in the ways specified in our proposed rule. See Proposed Rule § 64.1708(d). We do not, for example, request a time-stamp accurate to within 100 milliseconds indicating when a subscriber has pressed a key on a wireless telephone.

TIA also maintains that there is no deficiency in the interim standard because that standard provides for a time-stamp to be affixed when the triggering event is detected at the "intercept access point" (i.e., the point in the network used to access call-identifying information for the purposes of an intercept). See TIA Comments at 66-67. TIA does not explain how a standard can be thought to require an adequate level of accuracy when it in fact requires no particular level of accuracy.

Finally, BellSouth objects that it would be expensive to synchronize the carriers' switches to Universal Coordinated Time. See BellSouth Comments at 12-13. But we are not asking carriers to create such synchronization, and in fact the very purpose of our recommendation regarding the accuracy of the time-stamp is to make synchronization unnecessary. If law enforcement can be confident of the accuracy of the time-stamp to within 100 milliseconds, it can ascertain the difference between the time kept by the clock affixing the time-stamp on the call data channel, and

the time kept by the clock to which events on the call content channel are referenced, by comparing the time derived from each of these methods for the initiation of a call. Other events occurring during the call can then be correlated using this fixed time differential. If the accuracy of the time-stamp is not assured, however, it will be impossible for law enforcement to determine whether the differential should be ascribed to the difference between the two clocks' settings, or to delays between the event and the affixing of the time-stamp.

H. Automated Delivery of Surveillance Status Information

1. Section 103(a) of CALEA provides that a telecommunications carrier "shall ensure" that its equipment, facilities, and services are capable of isolating and delivering communications and call-identifying information to law enforcement. Section 103 thus places an affirmative obligation on the carrier to verify that its equipment is operational and that law enforcement has access to all communications and call-identifying information within the scope of the authorized surveillance. However, the interim standard does not contain any provisions that give effect to this affirmative statutory obligation.

To cure this deficiency, the government's petition proposes that the Commission add three elements to the interim standard: (i) a continuity tone, which would enable law enforcement to confirm that "all" (and not only a subset) of the communications subject to surveillance authorization and carried by a carrier to or from its equipment, facilities, or services were intercepted, CALEA § 103(a); (ii) a surveillance status message, which would record the activation, updating, and deactivation of any surveillance, as well as periodically signaling law enforcement that the surveillance is functional; and (iii) a feature status message, which would record any changes in a subscriber's call features and services. See DOJ/FBI Petition at 52-57. The commenters have failed

to refute either our assertion that the absence of any mechanism for providing surveillance status information represents a deficiency in the interim standard. or that our suggested methods for curing this deficiency should be included in the Commission's standards.

A few comments attempt to counter our fundamental assertion that the absence of any requirement for the delivery of surveillance status information represents a deficiency in the interim standard, but these comments misunderstand the nature of the relationship between the interim standard and Section 103. As explained above, Section 103 does not require any specific method of complying with its general assistance capability obligations. Thus, it is quite beside the point to argue that the specific requirements that we have recommended for inclusion in the Commission's rule are not expressly required by Section 103. Neither is it the case, as TIA suggests, that we are trying to insert "second-order obligations" into Section 103 (TIA Comments at 68); we are relying instead on a carrier's primary obligation under Section 103 to "ensure" that its equipment is capable of providing access to the information specified by CALEA. Because the interim standard fails to address this issue, these objections must be rejected.

2. As explained in the government's petition, law enforcement's ability to make effective use of information collected in an interception often depends on its ability to verify that all of the communications subject to surveillance authorization and carried by a carrier to or from its equipment, facilities, or services were intercepted during the relevant period. If law enforcement cannot verify that this is the case, a defendant could claim that non-intercepted communications undermined the significance placed on intercepted communications by law enforcement, for example by ascribing innocuous meanings to expressions that law enforcement describes as code words for

illegal activity. The government's proposed rule therefore provides for a "continuity tone" that will verify that the call content channels between the carrier and law enforcement are operational.

One commenter states that it "supports the use of a continuity tone if its use is limited to instances where dedicated content delivery channels from the switch to LEA locations are involved." BellSouth Comments at 15. This is precisely what the government is recommending. BellSouth's readiness to provide the precise capability that the government is requesting casts serious doubt on the representations by other commenters that providing this capability would be prohibitively complex or expensive.

A few commenters assert that this proposal represents an impermissible attempt by law enforcement to "dictate" the manner in which the industry complies with CALEA. SBC Comments at 13; AT&T Comments at 13; AirTouch Comments at 24. This assertion has nothing to do with the essential issue of whether the lack of such a provision in the interim standard constitutes a deficiency, and as we have explained above, it fundamentally misunderstands the nature of this proceeding. Furthermore, the government's proposal would not require any carrier to implement any particular design or equipment, because even carriers choosing to follow the Commission's standards may provide the continuity tone by means of any equipment they prefer.

One commenter argues that a continuity tone has "nothing to do with call identifying information or the content of communications." SBC Comments at 13. But the government does not contend that a continuity tone is itself call-identifying information or call content; instead, it is a means of satisfying the carrier's obligation to "ensure" the effective delivery of such information. The information provided by a continuity tone is absolutely essential to law enforcement's ability to make effective use of electronic surveillance. Without such a means of attesting to the continuous

functioning of an intercept, law enforcement's ability to use information gathered through electronic surveillance to build cases against criminals is severely undermined. This is why law enforcement has always created its own continuity tones when conducting pre-digital wiretaps -- because this verification capability in fact has everything to do with the effective use of legally-authorized surveillance.

PrimeCo warns that a carrier "cannot reasonably be expected to monitor whether the delivery channels [leased by law enforcement from a local exchange carrier] have failed." PrimeCo Comments at 20; see also AirTouch Comments at 25. The government certainly does not seek to hold a carrier responsible for the maintenance of a continuity tone over lines that it neither controls nor has contracted to utilize, and a carrier would not lose the protection of the safe harbor because the continuity tone was interrupted due to a flaw in a system for which they are not responsible. However, there is no logical reason to excuse a carrier from providing a reliable tone simply because it has contracted for the use of lines, rather than using only its own lines.

PrimeCo also states that circuits already have "special tone or idle pattern[s]," and suggests that law enforcement simply make use of these. PrimeCo Comments at 20. The government has no objection to the use of existing tones or idle patterns, and would accept the use of any already-existing tones or patterns that could match the functionality of the continuity tone that we have described. To reiterate, our principal purpose is neither to seek to require particular methods of complying with Section 103, nor even to require particular methods of curing the deficiencies that we have identified in the interim standard. If carriers can provide the Commission with other, equally effective methods of curing these deficiencies, the government has no objection to the use of such methods.

Some commenters object that providing law enforcement with a continuity tone would require expensive modifications of existing switches. TIA Comments at 69; AirTouch Comments at 24. To the extent that these commenters are simply relying on cost considerations, their objections may be relevant to relief under Section 109(b) but are not relevant to the scope of a carrier's underlying obligations under Section 103. See p. 35 supra. In any event, providing a continuity tone or its equivalent should require no major modifications of existing systems, because carriers already use digital bit patterns for maintenance oversight on their trunk lines. The government has no objection to carriers using these same features to provide the functional equivalent of a continuity tone. The Commission is free to consider any alternative means of curing this deficiency that would be more acceptable to the industry than the continuity tone while providing the same functionality.

3. The interim standard also fails to give law enforcement a means of determining whether interception software is accessing the correct equipment, service, or facility. The government's petition and proposed rule seek to cure this deficiency by including a provision for the automated delivery of surveillance status messages, which would indicate that the interception is working correctly and is accessing the correct subscriber's service. This provision would implement the requirement in Section 103 that a carrier "shall ensure" that its facilities are capable of delivering the surveillance information that law enforcement has requested through a court-authorized interception, as well as ensuring that law enforcement can make effective use of this information.

US West argues that Section 103's "shall ensure" language merely "impl[ies] a duty to provide reliable electronic surveillance service." US West Comments at 23. US West does not explain how a carrier that leaves law enforcement in the dark as to whether its intercepts are properly connected, functioning, capable of collecting all of the information crucial to an investigation, and

attached to the proper individual's lines could nevertheless be thought to provide "reliable electronic surveillance service." Nor does it attempt to counter our observation that, without the surveillance status information that we have described, law enforcement will be unable to make use of the surveillance information it collects. The "shall ensure" language in Section 103 reinforces a fundamental fact that neither this nor any other commenter can undermine: law enforcement must be able to monitor the status of its surveillances in order to make effective use of legally-authorized interceptions.

PrimeCo argues that a more reasonable method for law enforcement to verify whether a wiretap is operational would be to "perform a periodic trap and trace test of the target's phone number to verify that it is working." PrimeCo Comments at 20. PrimeCo apparently means to suggest that law enforcement should place periodic calls to the subject's phone, each time perhaps pretending that it had dialed a wrong number, and evaluate the soundness of the interception during these calls. Aside from being absurdly contrary to the common-sense notion that surveillance should be as unobtrusive as possible, this "solution" would violate the specific mandate of Section 103(a)(4) of CALEA, which requires that interceptions be conducted "unobtrusively" and "in a manner that protects * * * information regarding the government's interception of communications and access to call-identifying information."

TIA asserts that providing a surveillance status message would be unduly burdensome and costly. See TIA Comments at 70. This comment effectively rests on the premise that carriers have no mechanism in place for determining whether any or all of the circuits that make up their networks are functioning. Of course, carriers have such mechanisms in place, and without them they would be unable to conduct their business. Many have worked extensively to develop these infrastructures

in cooperation with Subcommittee T1M1 and the TR45.7, in an effort known as the Telecommunications Management Network.

The optional "connection test message" of the interim standard is not, as one commenter claims (see USTA Comments at 6), sufficient to meet law enforcement's need for surveillance status information. The first reason for its inadequacy is that it is optional, and thus carriers are not required to provide it at all. Second, unlike the government's proposal, the connection test message comes with no "triggers," or meaningful junctures at which the relevant information would be delivered. Finally, the connection test message contains no assurance to law enforcement that its intercepts are properly provisioned in the network, meaning that it is incapable -- for example -- of alerting law enforcement to the fact that an intercept is attached to the wrong subscriber's line.

BellSouth notes that various distribution architectures will require diverse solutions for the provision of surveillance status information. BellSouth observes that in the cellular context, for example, surveillances are necessarily distributed (because a subject may move from one cellular transmitter and its respective switch to another during a single communication). See BellSouth Comments at 13. We agree. Once again, we stress that our main concern is that the deficiencies we have identified in the interim standard be corrected. We have repeatedly noted that our specific suggestions for correcting these deficiencies might not represent the only available means for doing so. In this context, we are open to any solution that proves convenient for carriers dealing with various distribution architectures while preserving the functionality required by Section 103. If, for example, a cellular carrier finds it more convenient to aggregate information from dispersed locations into a single surveillance status message, we could support that solution if it were to promise a functionality sufficient to satisfy Section 103's requirements.

AT&T suggests that "human intervention" is adequate to cure the deficiency identified by the government. See AT&T Comments at 13. This suggestion is entirely at odds with the present-day reality of "human intervention." Law enforcement has attempted to obtain this information by calling carriers and asking them to send technicians to check on intercepts, but has found this process to be extremely ineffective. Faced with rapidly-unfolding events in an investigation, law enforcement often finds itself desperately in need of assurances with regard to the status of a wiretap at odd hours, when none of the carrier's technicians is available to conduct the necessary checks. Hiring the number of technicians necessary to meet law enforcement's needs, and paying them to be available around the clock (as automated status reporting systems are), would be far from a cost-effective solution, from the perspective either of the carriers or of law enforcement.

4. Finally, the interim standard does not require carriers to "ensure" that their equipment is capable of intercepting all information pertinent to a legally-authorized interception by enabling law enforcement to know when and how the calling features and services available to a subscriber have changed. As a means of curing this deficiency, the government's petition and proposed rule include a provision for the automated delivery of a feature status message that would notify law enforcement of such changes.

TIA states that it is unclear whether we are suggesting that law enforcement be informed whenever a subscriber requests a change in service, or rather only when a change in service becomes effective for a subscriber, and argues that the former requirement would be burdensome to implement. See TIA Comments at 70-71. We propose only the latter requirement, and thus TIA's arguments regarding the feasibility of the former are irrelevant. By mounting no challenge to the